Model suggests when it is best to blame someone for a cyber-attack or when to keep quiet about it

February 28 2017, by Bob Yirka

Hack attack. Wikipedia, CC BY-SA

(Tech Xplore)—A team with researches from several institutions in the U.S. has built a model to help decision makers decide when it is best to

keep quiet about a cyber-attack or when to publicly blame those suspected of carrying out the attack. In their paper published in *Proceedings of the National Academy of Sciences*, the team describes scenarios in which game theory can help those in a position to take action against hackers.

Getting hacked has become commonplace in the world today, particularly for public and private institutions. The damage from a cyber-attack can include identity theft, public embarrassment, and altering the outcome of a nationwide election. In this new effort, the researchers have found that game theory suggests publicly blaming those believed to be responsible for an attack may not always be the best course of action.

One example would be where an attacker has been identified but the victim has little means of recourse—The North Korean hack into Sony's database is such an example. Successfully stealing secrets from Sony was nothing but positive for North Korea, but because the country has little to hack, publicly announcing that they were the perpetrators only served to bolster that country's tech cred. The same might be said for a Russian team hacking into emails of Democratic Party leaders in the U.S.—when it was discovered who had done the deed, those who had been wronged took to the press to argue for revenge. Yet the only fallout appeared to be chest thumping by people all over Russia—even President Obama noted at the time that perhaps revealing the perpetrators only served to instill pride in the Russian people and their gang of hackers.

Looking at it from the other side, there are clear cases when going public is the best course of action—when hackers broke into the accounts of celebrities, stole private pictures and posted them on the internet, the publicity surrounding the event helped to finger those responsible—when the perpetrators were caught and sentenced to jail, it sent a very clear message to others who might be considering something similar.

Some have likened the business of government-sponsored hacking attacks as a new form of modern warfare and smaller attacks by angry groups as terrorism. This, the researchers suggest, means that groups or governments will need to have more tools available, such as the model they have built, to make better decisions when deciding how to retaliate under sometimes murky circumstances.

More information: Benjamin Edwards et al. Strategic aspects of cyberattack, attribution, and blame, *Proceedings of the National Academy of Sciences* (2017). DOI: 10.1073/pnas.1700442114

Abstract
Cyber conflict is now a common and potentially dangerous occurrence. The target typically faces a strategic choice based on its ability to attribute the attack to a specific perpetrator and whether it has a viable punishment at its disposal. We present a game-theoretic model, in which the best strategic choice for the victim depends on the vulnerability of the attacker, the knowledge level of the victim, payoffs for different outcomes, and the beliefs of each player about their opponent. The resulting blame game allows analysis of four policy-relevant questions: the conditions under which peace (i.e., no attacks) is stable, when attacks should be tolerated, the consequences of asymmetric technical attribution capabilities, and when a mischievous third party or an accident can undermine peace. Numerous historical examples illustrate how the theory applies to cases of cyber or kinetic conflict involving the United States, Russia, China, Japan, North Korea, Estonia, Israel, Iran, and Syria.

Press release